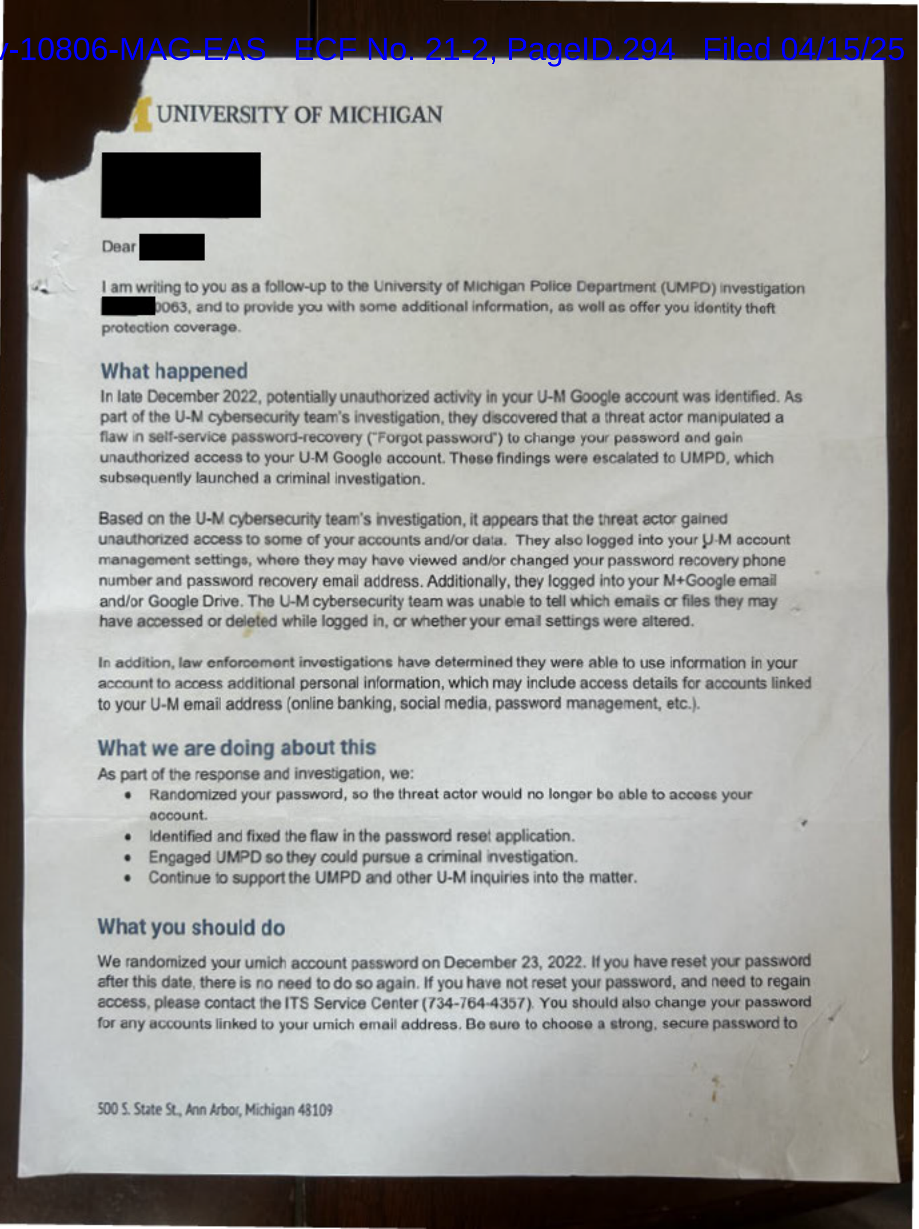
EXHIBIT A



UNIVERSITY OF MICHIGAN

[redacted]

Dear [redacted]

I am writing to you as a follow-up to the University of Michigan Police Department (UMPD) investigation [redacted]0063, and to provide you with some additional information, as well as offer you identity theft protection coverage.

What happened

In late December 2022, potentially unauthorized activity in your U-M Google account was identified. As part of the U-M cybersecurity team's investigation, they discovered that a threat actor manipulated a flaw in self-service password-recovery ("Forgot password") to change your password and gain unauthorized access to your U-M Google account. These findings were escalated to UMPD, which subsequently launched a criminal investigation.

Based on the U-M cybersecurity team's investigation, it appears that the threat actor gained unauthorized access to some of your accounts and/or data. They also logged into your U-M account management settings, where they may have viewed and/or changed your password recovery phone number and password recovery email address. Additionally, they logged into your M+Google email and/or Google Drive. The U-M cybersecurity team was unable to tell which emails or files they may have accessed or deleted while logged in, or whether your email settings were altered.

In addition, law enforcement investigations have determined they were able to use information in your account to access additional personal information, which may include access details for accounts linked to your U-M email address (online banking, social media, password management, etc.).

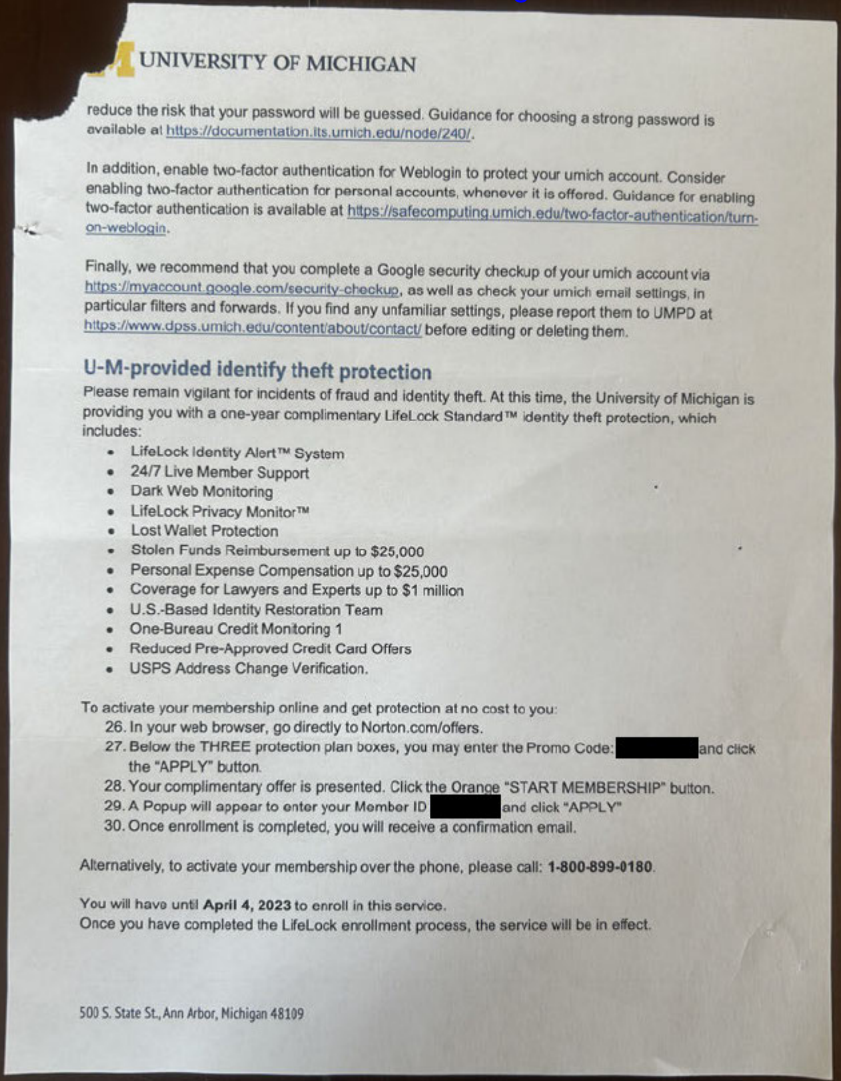
What we are doing about this

As part of the response and investigation, we:

- Randomized your password, so the threat actor would no longer be able to access your account.
- Identified and fixed the flaw in the password reset application.
- Engaged UMPD so they could pursue a criminal investigation.
- Continue to support the UMPD and other U-M inquiries into the matter.

What you should do

We randomized your umich account password on December 23, 2022. If you have reset your password after this date, there is no need to do so again. If you have not reset your password, and need to regain access, please contact the ITS Service Center (734-764-4357). You should also change your password for any accounts linked to your umich email address. Be sure to choose a strong, secure password to



UNIVERSITY OF MICHIGAN

reduce the risk that your password will be guessed. Guidance for choosing a strong password is available at https://documentation.its.umich.edu/node/240/.

In addition, enable two-factor authentication for Weblogin to protect your umich account. Consider enabling two-factor authentication for personal accounts, whenever it is offered. Guidance for enabling two-factor authentication is available at https://safecomputing.umich.edu/two-factor-authentication/turn-on-weblogin.

Finally, we recommend that you complete a Google security checkup of your umich account via https://myaccount.google.com/security-checkup, as well as check your umich email settings, in particular filters and forwards. If you find any unfamiliar settings, please report them to UMPD at https://www.dpss.umich.edu/content/about/contact/ before editing or deleting them.

U-M-provided identify theft protection

Please remain vigilant for incidents of fraud and identity theft. At this time, the University of Michigan is providing you with a one-year complimentary LifeLock Standard™ identity theft protection, which includes:

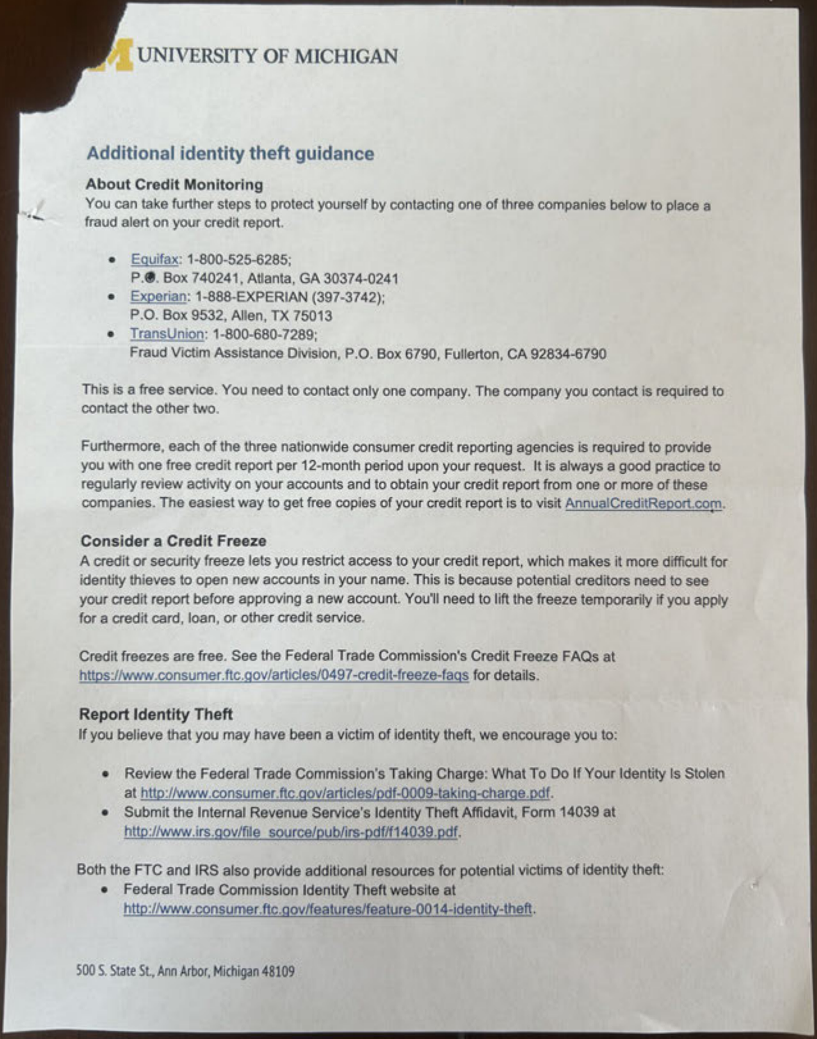
- LifeLock Identity Alert™ System
- 24/7 Live Member Support
- Dark Web Monitoring
- LifeLock Privacy Monitor™
- Lost Wallet Protection
- Stolen Funds Reimbursement up to $25,000
- Personal Expense Compensation up to $25,000
- Coverage for Lawyers and Experts up to $1 million
- U.S.-Based Identity Restoration Team
- One-Bureau Credit Monitoring 1
- Reduced Pre-Approved Credit Card Offers
- USPS Address Change Verification.

To activate your membership online and get protection at no cost to you:

26. In your web browser, go directly to Norton.com/offers.
27. Below the THREE protection plan boxes, you may enter the Promo Code: [redacted] and click the "APPLY" button.
28. Your complimentary offer is presented. Click the Orange "START MEMBERSHIP" button.
29. A Popup will appear to enter your Member ID [redacted] and click "APPLY"
30. Once enrollment is completed, you will receive a confirmation email.

Alternatively, to activate your membership over the phone, please call: **1-800-899-0180**.

You will have until **April 4, 2023** to enroll in this service.
Once you have completed the LifeLock enrollment process, the service will be in effect.



UNIVERSITY OF MICHIGAN

Additional identity theft guidance

About Credit Monitoring

You can take further steps to protect yourself by contacting one of three companies below to place a fraud alert on your credit report.

- Equifax: 1-800-525-6285;
  P.O. Box 740241, Atlanta, GA 30374-0241
- Experian: 1-888-EXPERIAN (397-3742);
  P.O. Box 9532, Allen, TX 75013
- TransUnion: 1-800-680-7289;
  Fraud Victim Assistance Division, P.O. Box 6790, Fullerton, CA 92834-6790

This is a free service. You need to contact only one company. The company you contact is required to contact the other two.

Furthermore, each of the three nationwide consumer credit reporting agencies is required to provide you with one free credit report per 12-month period upon your request. It is always a good practice to regularly review activity on your accounts and to obtain your credit report from one or more of these companies. The easiest way to get free copies of your credit report is to visit AnnualCreditReport.com.

Consider a Credit Freeze

A credit or security freeze lets you restrict access to your credit report, which makes it more difficult for identity thieves to open new accounts in your name. This is because potential creditors need to see your credit report before approving a new account. You'll need to lift the freeze temporarily if you apply for a credit card, loan, or other credit service.

Credit freezes are free. See the Federal Trade Commission's Credit Freeze FAQs at https://www.consumer.ftc.gov/articles/0497-credit-freeze-faqs for details.

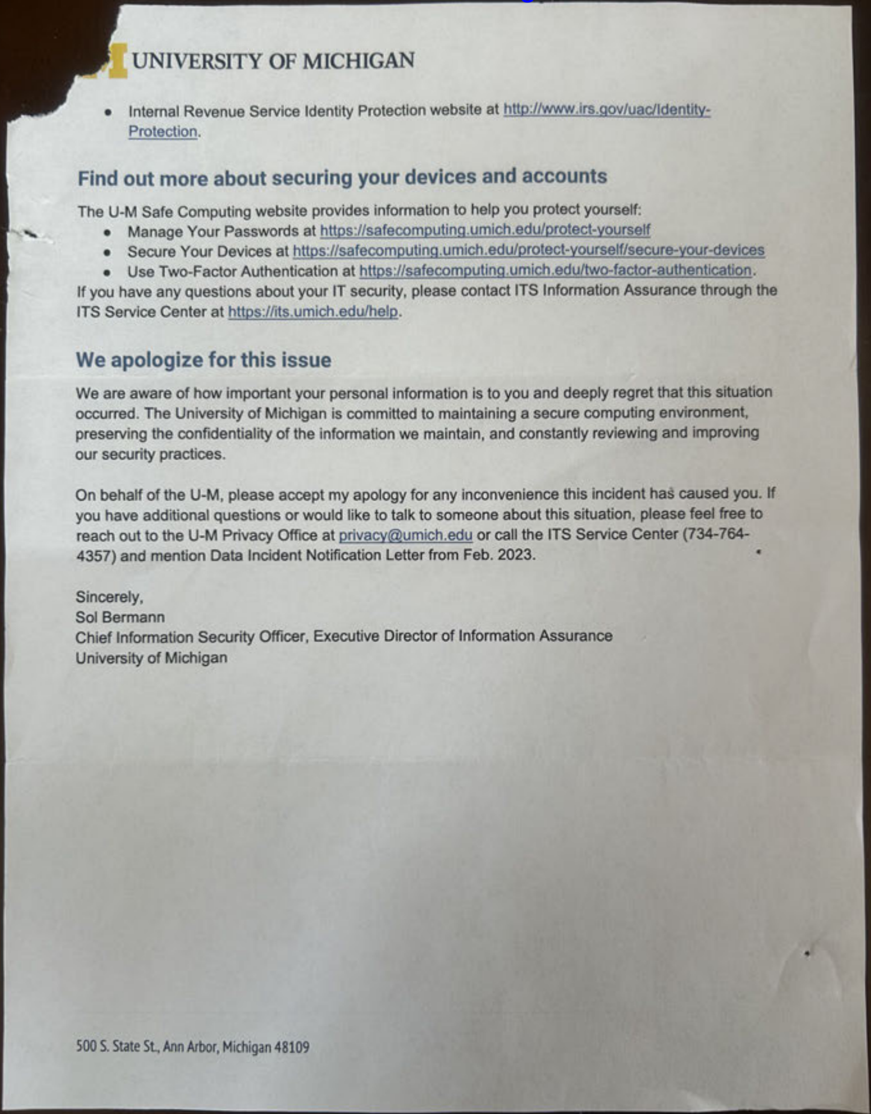
Report Identity Theft

If you believe that you may have been a victim of identity theft, we encourage you to:

- Review the Federal Trade Commission's Taking Charge: What To Do If Your Identity Is Stolen at http://www.consumer.ftc.gov/articles/pdf-0009-taking-charge.pdf.
- Submit the Internal Revenue Service's Identity Theft Affidavit, Form 14039 at http://www.irs.gov/file_source/pub/irs-pdf/f14039.pdf.

Both the FTC and IRS also provide additional resources for potential victims of identity theft:

- Federal Trade Commission Identity Theft website at http://www.consumer.ftc.gov/features/feature-0014-identity-theft.



- Internal Revenue Service Identity Protection website at http://www.irs.gov/uac/Identity-Protection.

Find out more about securing your devices and accounts

The U-M Safe Computing website provides information to help you protect yourself:

- Manage Your Passwords at https://safecomputing.umich.edu/protect-yourself
- Secure Your Devices at https://safecomputing.umich.edu/protect-yourself/secure-your-devices
- Use Two-Factor Authentication at https://safecomputing.umich.edu/two-factor-authentication.

If you have any questions about your IT security, please contact ITS Information Assurance through the ITS Service Center at https://its.umich.edu/help.

We apologize for this issue

We are aware of how important your personal information is to you and deeply regret that this situation occurred. The University of Michigan is committed to maintaining a secure computing environment, preserving the confidentiality of the information we maintain, and constantly reviewing and improving our security practices.

On behalf of the U-M, please accept my apology for any inconvenience this incident has caused you. If you have additional questions or would like to talk to someone about this situation, please feel free to reach out to the U-M Privacy Office at privacy@umich.edu or call the ITS Service Center (734-764-4357) and mention Data Incident Notification Letter from Feb. 2023.

Sincerely,
Sol Bermann
Chief Information Security Officer, Executive Director of Information Assurance
University of Michigan